

STRATEGY  
RESEARCH  
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

NATIONAL MILITARY STRATEGY: INFORMATION WARFARE

BY

LIEUTENANT COLONEL LARRY P. HALL  
United States Army

DISTRIBUTION STATEMENT A:  
Approved for public release.  
Distribution is unlimited.

19970623 263  
807



USAWC CLASS OF 1997  
U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

DATA QUALITY INSPECTED 4

USAWC STRATEGY RESEARCH PROJECT

**NATIONAL MILITARY STRATEGY:  
INFORMATION WARFARE**

BY

LTC Larry P. Hall

Mr. Robert Minehart  
Project Advisor

The views expressed in this paper are those of the author and do not necessarily reflects the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

DISTRIBUTION STATEMENT A:  
Approved for public  
release. Distribution is  
unlimited.

U. S. Army War College  
Carlisle Barracks, Pennsylvania 17013

## ABSTRACT

AUTHOR: Larry P. Hall (LTC), USA

TITLE: National Military Strategy: Information Warfare

FORMAT: Strategy Research Project

DATE: 7 April 1997 PAGES: 26 CLASSIFICATION: Unclassified

### Information Warfare

The U. S. Government has realized that new technologies will have a significant impact not only on everyday life but also on national security and the conduct of future warfare. While evaluating the powerful potential of information, policymakers are also attempting to understand a variety of problems surrounding it. This paper analyzes IW, specifically the protection of information, as a component of the 1995 National Military Strategy (NMS). It reviews the ends, ways, and means of our IW strategy. It focuses on the actions of the U. S. Government, the Department of Defense (DoD), and Joint Chiefs of Staff (JCS), especially on the U. S. Army's role. It examines the Army's IW strategy and provides some recommendations for what it needs to do to further support national policy.

## TABLE OF CONTENTS

ABSTRACT.....	iii
INTRODUCTION.....	1
NATIONAL POLICY.....	2
DoD POLICY.....	3
THE THREAT.....	3
POLICY INTO ACTION.....	6
JOINT CHIEFS OF STAFF ACTION.....	10
ARMY ACTION.....	12
RECOMMENDATIONS.....	19
CONCLUSION.....	23
ENDNOTES.....	25
SELECTED BIBLIOGRAPHY.....	27

## **NATIONAL MILITARY STRATEGY - INFORMATION WARFARE**

### **INTRODUCTION**

The Bible warns in the book of Proverbs that “A wise man will hear and increase learning, and a wise man of understanding will attain wise counsel, ... but fools despise wisdom and instruction.”<sup>1</sup> Taking heed of such advice, U. S. leaders have begun to develop policy addressing the myriad of problems surrounding the explosion of information. Few of us realize how information dependent we are becoming. This may leave us vulnerable to breakdowns in the information systems that we may unknowingly rely on. For example, effective Information Warfare (IW) could shut off our electricity, randomly jeopardize our credit rating, or disseminate misinformation to us on our Internet homepages. The time has come for us to prepare a more systematic defense against such insidious attacks.

The U. S. Government has realized that new technologies will have a significant impact not only on everyday life but also on national security and the conduct of future warfare. While evaluating the powerful potential of information, policymakers are also attempting to understand a variety of problems surrounding it. This paper analyzes IW, specifically the protection of information, as a component of the 1995 National Military Strategy (NMS). It reviews the ends, ways, and means of our IW strategy. It focuses on the actions of the U. S. Government, the Department of Defense (DoD), and the Joint Chiefs of Staff (JCS), especially on the U. S. Army’s role. It examines the Army’s IW strategy and provides some recommendations for what it needs to do to further support national policy.

## **NATIONAL POLICY**

President Clinton's 1996 National Security Strategy of Engagement and Enlargement (NSS) clearly recognizes the challenge facing America to learn about worldwide capabilities and emerging information technologies or infrastructure that may potentially threaten U. S. interests at home or abroad.<sup>2</sup> It expressly acknowledges the need to identify emerging threats to modern information systems and supports the development of protection strategies.<sup>3</sup> The NMS, in concert with the NSS, also cites the rising significance information will play in future warfare. The ability to fight and win the Nation's wars remains the foremost responsibility and prime consideration of all military activity. Accordingly, the NMS states that in war U. S. forces will be employed consistent with certain principles. One of the principles to achieve the end of defending the nation is to help dominate combat operations by winning the information war.<sup>4</sup> To support this objective, the NMS allows for the enhancement of military capabilities. In order to dominate warfare, these enhancements must provide advanced information technologies such as reconnaissance, intelligence collection and analysis, and high-speed data processing and transmission systems. We must assure that this leverage works for us and against our adversaries.<sup>5</sup> The NSS and NMS establish a useful policy that provides a beginning for America to understand the information threat and thereby provide the means to protect important facets of American life.

## **DoD POLICY**

The Department of Defense (DoD) has begun to develop strategies to address information operations based on national policies. In 1996, the Secretary of Defense issued his Annual Report to the President and the Congress in which he recognizes the importance of information and offers an overview of how our forces must be prepared to confront a wide range of potential opponents in a changing global environment.<sup>6</sup> IW is a worldwide problem: All industrial and information-age nation states face potential opponents who have access to a global market containing a vast array of modern technology.<sup>7</sup> IW offers a cheap and easy way for less developed countries, zealots, and hackers to anonymously mount an attack on another nation, corporation, institution, or person. Few if any nations would challenge the U. S. force on force. Therefore, America by eliminating the foreign military option has opened itself up to IW. The Revolution in Military Affairs (RMA) combines fielded and emerging technologies with organizational and operational changes. This RMA has the potential of producing dramatic improvements in military effectiveness. DoD recognizes that this change can be profound, and that the new methods of warfare can be far more powerful than the old.<sup>8</sup> Acknowledging the threat, DoD understands the priority to protect the effective and continuous operation of military and commercial information systems.

## **THE THREAT**

Martin Libicki, a Senior Fellow at the National Defense University Institute of Strategic Studies, in What is Information Warfare makes the point that information and

its technologies are increasingly important to national security in general, and to warfare specifically. He states that advanced conflicts will be increasingly characterized by the struggle over information systems. America, as the world's preeminent information society, could increase its advantage over any opponent if it takes IW seriously. However, if it fails to do so, it may face a considerable disadvantage, regardless of strengths in other military dimensions.<sup>9</sup> In evaluating the IW threat, we should consider not only the electronic or radio frequency vulnerabilities, but also attacks on computers, the information on computers, and the components that control the critical infrastructure on which our systems depend. Similarly, the threat of physical damage to equipment and property is just as real and significant. But what cause have we for these concerns? Is America really vulnerable?

The Director of Central Intelligence (DCI), John Deutch, has called the electron "the ultimate precision-guided weapon."<sup>10</sup> He told a Senate hearing that he was convinced that there is a growing awareness around the world that advanced societies, especially the U. S., are increasingly dependent on open and potentially vulnerable information systems. He indicated that his greatest concern was that hackers, terrorists, or other nations could use easily acquired software and hardware to seriously disrupt electric power distribution, air traffic control, financial sectors, international commerce, and military forces. He also indicated that the IW threat from both state and non-state actors will grow over the next decade as the technology proliferates. Although most of the numerous intrusions into critical information systems have so far come from "hackers" and criminals, U. S. intelligence estimates that many terrorist groups and over

120 nations are developing offensive IW capabilities.<sup>11</sup> It is easier for under-developed countries to steal intellectual and proprietary property than to invest in time and resources to develop their own.

Senator Jon Kyl (R-Arizona) has warned "that there is at present, no defense against invasions of the nerve centers of our society, which include our defense, telephone, public utility, and banking systems. Top U. S. officials are recognizing their lack of preparedness for what some call the cyber equivalent of Pearl Harbor."<sup>12</sup> Attorney General Janet Reno has said "as businesses, government, and individuals increasingly rely on computers to communicate and store vital information, terrorists could use more sophisticated cyber attacks on computer and communications systems to disrupt the functioning of the nation's critical infrastructures."<sup>13</sup> She knows. This past August hackers replaced her as the attorney general on the Department of Justice's (DOJ) Web pages with the likeness of Adolf Hitler. The need to increase public awareness is important in protecting both access to the Web sites and the information itself. Americans should beware. We cannot afford to overlook security issues at the expense of information availability and rapid accessibility.<sup>14</sup> As Web sites are created to quickly get information on line, the protection of that information must always remain a priority.

Pentagon computers are often common targets; and they are vulnerable. Over the December 28-29 weekend, the Pentagon denied public access to most of its computer Web sites once officials found that the Air Force World Wide Web homepage had been altered. The Defense Technical Information Center (DTIC) at Fort Belvoir, Virginia manages 80 DoD Web sites. It decided to temporarily take all servers off line after the

damaged file was discovered.<sup>15</sup> The DTIC provides the public unprecedented access to Pentagon news, information, plans and policies.” It also acts as a clearinghouse for DoD scientific and technical information.<sup>16</sup>

The General Accounting Office (GAO), the investigative arm of Congress, reported last spring that Pentagon computers are attacked as many as 250,000 times each year. The GAO report also suggests that the “potential for catastrophic damage is great,” noting that these attacks are successful about 65 percent of the time and that the number of attacks is doubling every year.<sup>17</sup>

Private industry is particularly vulnerable. A survey conducted by Warroom Research, Inc., shows that 58 percent of the 236 companies it polled had been hit by hackers in the previous 12 months. During this period, some 57 companies were violated and broken into at least 11 times. The November 1996 study states that hackers, broke into corporate networks, installed on-line eavesdropping devices called “sniffers,” copied secret passwords, inserted destructive computer viruses, and stole secret business data.<sup>18</sup>

## **POLICY INTO ACTION**

American policymakers have begun to develop the ways to understand and thus to protect “information” from various threats. The National Intelligence Council (NIC) produced a classified report last summer on foreign IW plans and programs. NIC was directed by the DCI to build on this report in collaboration with domestic and military agencies to produce a National Intelligence Estimate, an official guide for policymakers.<sup>19</sup>

In an effort to address IW with other conventional threats, the DOJ has brought together the government, military, and business communities to serve on a new Presidential Commission on Critical Infrastructure Protection. The commission's formation was announced in August; it will prepare a report within a year. In the interim, the president has ordered the establishment of an inter-agency Infrastructure Protection Task Force, chaired by the FBI.<sup>20</sup> This Task Force will bring the real issue before the nation. IW is not just computer warfare. It is really much more, it approaches infrastructure warfare. IW is not particularly interested in an adversary's computer; IW attacks what the computer does or controls. IW can jeopardize power grids, financial centers, personnel records, air defense systems, command and control nodes, and transportation hubs. Our military should illuminate these aspects of IW so that the civilian sector better understands the real IW threat.

Winning the information war is a clearly defined objective of the NMS. Consequently, the DoD has aggressively developed a concept to accomplish that end. The Deputy Secretary of Defense has recently published a new DoD Directive 3600.1. This update, "Information Operations and Information Warfare" significantly changes the old directive. It notes that rigorous steps have been undertaken to understand Information Operation (IO) activities, previously referred to as IW, which is now included as a subset of IO. This change helps to de-militarize the terminology while educating and hopefully securing civilian sector support. After three years of study and support from the DoD community, the new concepts are sufficiently refined to update DoD guidance. DoD

also recognizes that our collective understanding of this concept continues to evolve. It expedited publishing the new directive in order to get on with IO implementation.<sup>21</sup>

The Defense Intelligence Agency has been tasked to provide detailed assessments of critical nodes and information infrastructures to support deliberate planning and target selection for various scenarios. Service schools are introducing IW into their curricula, and IW issues are being integrated into wargame scenarios and in modeling and simulation initiatives.<sup>22</sup>

Advanced Concept Technology Demonstrations (ACTDs), a concept designed to accelerate the transition of maturing technologies into improved military capabilities, have also begun to include emerging IW technologies into testing and exercises. ACTD provides a means to rapidly move new and proven IW capabilities to operational forces. This rapid transition of emerging technologies from the laboratory into the field facilitates the timely outfitting of operational units. It will allow them to operate safely and effectively in today's volatile, uncertain, complex, and ambiguous (VUCA) environment.<sup>23</sup>

Joint Warrior Interoperability Demonstration (JWID) is an annual series of technology demonstrations designed to encourage innovative solutions to challenges faced by the U. S. military. These exercises test concepts, hardware, training techniques and doctrinal issues. JWID '96 was coordinated by the Commander of the U. S. Central Command and led by the U. S. Army. It tested 45 separate technologies, to include those associated with IW. The IW demonstrations focused on improving joint command, control, communications, computers and intelligence (C4I). Unique to this JWID was the

attack of many information systems by information warfare teams from the Defense Information Systems Agency (DISA). This demonstration of technologies, followed by an evaluation of successes and failures, will likely affect future acquisition decisions.<sup>24</sup>

As the above examples show, policymakers have begun to respond to IW issues: They have launched an array of initiatives or ways to ensure protection of our information systems.

Our leaders have also provided adequate resources or means to protect America's effective and continuous operation of information systems, whether it be people, organizations, funds or technology. The DCI, announced in July 1996 plans to establish a cyberwar center at the National Security Agency (NSA) in order to protect the country's network infrastructures.<sup>25</sup> According to a staff report by the Senate Permanent Subcommittee on Investigations, the NSA IW Center will focus on both offensive and defensive measures.<sup>26</sup> The Electronic Industries Association estimates that over the next decade the government's information warfare procurement will grow sevenfold to more than \$1 billion annually.<sup>27</sup> Sarah Jean League, the special assistant to the Defense Information Systems Agency and DoD for the Presidential Commission on Critical Infrastructure Protection, stated at a September 1996 conference that the DoD will spend more than \$1 billion over the next five years to defend U. S. systems.<sup>28</sup>

The Wall Street Journal reported on 6 January 1997 that the DoD has recommended establishing a new "information warfare" czar. A Defense Science Board task force also released a report calling for \$580 million in research and development spending over the coming years. To be spent primarily in the private sector, these funds

would support development of new software and hardware to provide security, such as a system for automatically tracing hacker attacks back to their source. The Wall Street Journal also reported that the task force recommended changing laws to allow the Pentagon to legally pursue and repel any parties attempting to hack into DoD computer systems.<sup>29</sup>

The Office of the Assistant Secretary of Defense (Command and Control Communications and Intelligence) (ASD(C3I)) has been designated the central DoD point of contact to establish IO policy and provide guidance and program oversight. ASD(C3I)'s duties also include centralized planning, coordination, and cross-service IO program management. In conjunction with the Under Secretary of Defense for Policy, ASD(C3I) will ensure IO coordination with other federal agencies and the civilian community. Roger Callahan, the ASD(C3I) director for information security, has already identified Pentagon officials as no longer referring to the protection of information as "information security" but as "information assurance" instead.

## **JOINT CHIEFS OF STAFF ACTION**

The Chairman of the Joint Chiefs of Staff (CJCS), General John M. Shalikashvili, states in Joint Vision 2010 that information superiority is necessary for joint military operations to succeed.<sup>30</sup> In a brochure recently published by the JCS, titled Information Warfare -- A Strategy for Peace...The Decisive Edge in War, General Shalikashvili notes that "IW has emerged as a key joint warfighting mission area" and that "the explosive proliferation of information-based technology significantly impacts warfighting across all

phases, the range of military operations, and all levels of war.” The Chairman also provides notice that “our reliance on technology creates dependency throughout our global basing and information support networks and generates requirements for defensive IW capabilities.” He further cautions that “the same technologies also create vulnerabilities” and has therefore initiated action to protect our forces and ensure we are not exploited by our adversaries.<sup>31</sup>

The JCS is working hard to increase IW awareness throughout the military. They have developed a joint vision and formulated an IW implementation strategy to support joint warfighting. They have also published and distributed the above mentioned IW brochure “to outline basic IW concepts and summarize ongoing initiatives implementing those concepts.”<sup>32</sup>

The JCS understands the critical importance of protecting our information infrastructure systems. It is acutely aware that “potential adversaries are rapidly exploiting information and information system technologies” and that “many vital warfighting tasks are dependent upon information and information-based technologies. Warfighting information systems are linked through supporting public infrastructures, thus exposed to attacks by a broad range of adversaries whose motives may be difficult to measure. Therefore, the difficulty in defending systems and processes upon which our warfighting capability depends is increased, and their defense is absolutely essential.”<sup>33</sup> In developing their defensive IW (IW-D) strategy, the JCS seeks to protect and defend information systems.

IW-D actions are those that “must be carefully considered, integrated at all levels of war, and applied across the range of military operations.” The JCS acknowledges the “requirement for IW-D to be organized as a system and tied together by policy, doctrine, technology, capability assessments, education, training, exercises, and a mutually supporting national organizational infrastructure.” While the JCS has focused on “specific aspects of policy and standards” of this system, it has also identified “five critical components that should be included in any attempt to implement an IW-D system.” These are “integrity, authentication, non repudiation, availability, and confidentiality.” JCS IW-D “implementation is designed with an objective of information assurance to protect access to timely, accurate, and relevant information wherever and whenever needed.”<sup>34</sup>

Committed to IW, the JCS has provided policy positions and designated responsibility in CJCS policy documents. “The Joint Staff has revised existing policy and developed new IW guidance when necessary. The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3210.01, established Joint IW Policy to support warfighting and CJCSI 6510.01A established Defensive Information Warfare Implementation, focusing on key areas of protecting and defending information systems.”<sup>35</sup>

## **ARMY ACTION**

The U. S. Army is not coming up short during this age of information explosion. It too understands the threat, both to the country and to itself. The Army knows that adversaries will seek potential IO advantages. Following the lead of the JCS, the Army

has developed an aggressive program to better understand the essence of IO and to determine how its organizations can benefit from it. General Dennis Reimer, the Chief of Staff of the Army (CSA), has stated that “victorious military operations demand the successful conduct of IO” and that “there are few greater challenges facing us today or in the future.”<sup>36</sup> The Army clearly recognizes the importance of IO and foresees the major impact these types of operations will have on Army warfighting capabilities of the future.

Joint Vision 2010 provides the services with a view of the future and the implications for joint operations. Therefore, the CSA in Army Vision 2010 further identifies the operational imperatives and enabling technologies required by the Army to contribute to joint operations. These fundamental competencies should allow the ground component commander to conduct “prompt and sustained operations on land throughout the entire spectrum of crisis and thus achieve full spectrum dominance.”<sup>37</sup> Army Vision 2010 provides a directional azimuth and seeks to support Joint Vision 2010 by assisting in the sizing, organizing and equipping of the Army, and in developing the doctrine for land force operations.<sup>38</sup>

In the quest for full spectrum dominance Army Vision 2010 has keyed on various tasks that armies have always performed in war and other military operations. Of particular note is the focus on Protecting the Force and Gaining Information Dominance.<sup>39</sup> To carry out these tasks, the Army of the future will exploit many new technologies in order to provide full dimensional protection not only for soldiers, but also for information and vital information infrastructure systems. The CSA emphasizes that it is key “to create a disparity between what we know about our battlespace and operations

within it and what the enemy knows about his.” The Army will target IO technologies to assist in understanding the battlespace “while disrupting and denying information to the enemy.”<sup>40</sup> Army leadership has deemed IO as essential to all operations and has therefore, through Army Vision 2010, challenged the different battlefield operating systems (BOS) to integrate IO into their plans for the 21st century.

As a large and diverse organization, the Army depends and functions primarily on doctrine. Doctrine determines how the Army trains and fights. Doctrine also drives the Army to establish requirements. These requirements then determine the capabilities necessary to accomplish the Army mission. Consequently, they determine how the Army modernizes. The Army, like the JCS, has fixed responsibilities, established priorities, identified resources, and published documents to provide credibility to its IO commitment. Field Manual 100-6 (FM 100-6), Information Operations, delineates ways to implement IO policy. Published in the summer of 1996, it establishes the Army doctrine for taking every measure to win the information war. It provides clear guidance for gaining information dominance. The doctrine found in FM 100-6 is consistent with General Reimer’s intent to provide an IO concept which “envision[s] a full spectrum force capable of decisive victory through the rapid attainment of campaign objectives with minimal risk to our most valuable assets...our soldiers.”<sup>41</sup>

We understand that today’s often invisible IO threat is very much different from traditional threats. Since this IO threat may be increasing daily, the CSA has placed a near-term priority on implementing the Army’s information assurance plan. To accomplish this, he created an Army IO triad. It consists of the deputy chief of staff for

operations and plans (DCSOPS), the deputy chief of staff for intelligence (DCSINT), and the director of information systems for command, control, communications, and computers (DISC4). With the DCSOPS as the lead element, they are responsible for implementing the CSA's "intent for IO and developing an IO campaign plan to incorporate, synchronize and conduct IO throughout the force." General Reimer has also directed that IO be "institutionalized through requirements definition, education, and training at Army schools and centers." Meanwhile, the Army will continue to "develop and refine IO doctrine and tactics, techniques, and procedures at the combat training centers."<sup>42</sup>

This IO triad has developed a command and control (C2) protection program. It applies and integrates all necessary operational, technical engineering, security disciplines and intelligence-counterintelligence into a protection program known as C2 Protect. While seeking to guard against potential threats, it also addresses various protection schemes -- from the national command authorities to the foxhole. Lieutenant General Otto J. Guenther, the DISC4, says that the Army's C2 Protect program management plan "provides the strategy for development and implementation of information protection measures."<sup>43</sup> Its focus is to maintain confidentiality and integrity; however, it is equally as important for C2 Protect to make the information necessary for decision making and control of forces and systems available.<sup>44</sup>

To be successful C2 Protect must identify and accomplish key tasks. The DISC4 highlights these tasks as "identifying IW elements as force multipliers, synchronizing current and planned IW activities, supporting education training and awareness, and

developing measures to provide effective C2 advantages.” He also relates that C2 Protect needs to “provide guidance for modernizing the force within the IO technical architecture’s framework.” In order to effectively address the vulnerabilities inherent in the Army’s information infrastructure, he calls for “a single unified vision of Army command, control, communications, computers and intelligence (C4I).” C2 Protect coordinates efforts related to information assurance and reliability and provides guidance on what the Army must do to ensure that its portion of the defense information infrastructure is adequately protected.<sup>45</sup>

The Land Information Warfare Center (LIWA), a bold initiative, offers more evidence of the Army’s emphasis on IO, especially on information assurance. Formed “out of hide” in 1994, the LIWA operates within the scope of intelligence, operational security and electronic warfare functions. Its director, Colonel Halbert F. Stevens, has observed that “although the LIWA is located within, and the people come from, the Intelligence and Security Command (INSCOM), the command belongs to operations. The LIWA is not an intelligence function; it is instead an operations organization, working for the DCSOPS.”<sup>46</sup> Indeed, the DCSOPS oversees the LIWA’s efforts in various military operations as commanders integrate IO into exercises, operational plans and orders.

Preserving and institutionalizing IO into the Army’s modernization plan and assuring land force dominance into the next century are key tasks for the LIWA. To assist commanders in planning operations, the LIWA, consistent with the Army’s desire for centralized planning and decentralized execution, will provide a small supporting staff

to augment primary staffs. Working with the commander's G-3 operations section, the field support teams have been designed to provide tailored IO support to land component commanders. The team usually consists of subject matter experts in such key areas as operational security, information security, computer security, and electronic warfare.

The LIWA is also the lead agency in the Army IW Red Team effort during certain exercises, planned tests, or demonstrations. This team seeks to determine whether an adversary's IW proficiency can be used against an identified U. S. vulnerability.<sup>47</sup> The Red Team attacks friendly systems, seeking out realistic vulnerabilities. Once the team disrupts the flow of information or successfully penetrates a system, it begins to assess perceived vulnerabilities. Then it assists in developing protection mechanism solutions.<sup>48</sup>

Colonel Stevens is keenly aware that assurance involves defending one's own information, information-based processes, information systems, and computer-based networks. Consequently, the Army and the LIWA focus on helping to integrate and protect automation and electronic systems such as navigation aids, position location, communications, networks, space systems, flight controls, sensor-to-shooter, data links, and data bases. Stevens contends that "there are relevant information elements that are critical to the commander's ability -- friendly information systems and friendly information force requirements that impact on a commander's capability." He clearly understands the threat: "Information systems are not just communications and computer hardware, but also the people and the organization necessary to push the information around the environment."<sup>49</sup>

The Military Intelligence Corps, one of the Army's battlefield operating systems (BOS), has contributed to helping the Army's information assurance posture. It developed, Intel XXI, Vision for the 21st Century to provide for future intelligence support. Working to assist the Army IO triad in gaining information dominance, Intel XXI focuses on how Army intelligence forces can best support commander-driven requirements in the information age of the 21st century.<sup>50</sup> The value of intelligence resides principally in its ability to reduce uncertainty and provide a clearer picture of the battlefield. Intel XXI strives to give commanders the intelligence and targets they need, when they need them. It must also, as a part of providing or assuming information dominance, concurrently fulfill the requirement to protect friendly systems against enemy attacks.<sup>51</sup>

Intelligence is a key player in the Army's IO structure, especially as it attempts to identify potential vulnerabilities and prescribe affordable protective measures. Under Intel XXI, Army intelligence assets will be trained to reduce a commander's uncertainty by understanding the threat environment and to identify our own information-related vulnerabilities. They will integrate multi-disciplined information to protect high priority targets such as friendly command and control systems.

These examples demonstrate that the Army has put forth tremendous effort to comply with the IW policy presented by the JCS and our national policymakers. It has pinpointed the threat, created doctrine, fixed responsibilities, and established priorities. It has identified appropriate means or resources, to include senior Army leadership, while energizing the entire force in its effort to contribute to ensuring the protection of vital

information. National policymakers and the Army however, should examine certain issues before declaring that this difficult problem has been sufficiently addressed to provide adequately for our nation's security.

## **RECOMMENDATIONS**

The current NMS policy on IW seems to be adequate. U. S. Government agencies, the DoD, and JCS have identified the threat, fixed responsibilities, assigned tasks, and set priorities to adhere to policymaker guidance. The Army, too, has done many necessary things to prepare itself for winning the information war. However, added emphasis in a few areas could help bring the Army in closer compliance with policymaker guidance. Before we consider specific recommendations for the Army, let's review two important issues.

First, American leaders, both governmental and private sector, must work together to create a strategy for protecting information and assuring continuous operations of information-dependent systems. They also need to ensure our strategies of protection do not intrude unduly on personal privacy. Protecting our information systems and their supporting infrastructure should not overshadow the importance of individual freedoms and individual rights as guaranteed by our Constitution. It is paramount that these rights be considered and protected when determining the level and ways of providing essential assistance to the private sector.

Second, America's lawmakers must examine international laws and their effects on American business. The recent U. S. Encryption policy requiring the use of Trusted

Third Parties and key recovery technology offers a good example of the application of technology to formulate international community standards. Our global partners must understand the commitment America is making and therefore must be inclined to respect the laws and cooperate in mutual enforcement.

The Army has accomplished much while striving to construct a viable IO program. It must continue to work diligently and concentrate on a few key areas in order to remain current with the fluid IO situation. These areas of interest center around doctrine, training, and modernization.

Doctrine, as stated before, determines how the Army trains and fights. Therefore, it is essential that the Army develop IO doctrine that is current and effective. It must continuously evaluate its relevancy, since technology is evolving so rapidly. IO doctrine can be updated and enhanced by applying the lessons learned from planned exercises. However, the Army must look beyond its own exercises and move toward interfacing with our sister services and other government agencies. Thereby expanding the venue, the Army can learn much more about what it needs to protect. Gaining a better perception about the information environment, to include the threat, will help identify key vulnerabilities.

Army participation in joint ventures and programs greatly assist in developing effective doctrine. The use of different models and simulations will aid in evaluating the systems on which the Army depends. Since dependency can breed vulnerability, the Army must identify its critical information systems and facilities, even those that are non-governmental.

Doctrine can assist in changing existing attitudes. Everyone should learn that interference with information is not just a crime -- but an act of war. Doctrine must address how soldiers should engage intruders and thus employ legal and proper procedures to provide assurance of critical data links and nodes. Responsibilities must be fixed. Doctrine must maximize the utilization of all Army assets. Scarce resources can be further strained by duplication of missions or tasks. Understanding its limitations, the Army can seek to capitalize on its own unique elements, but especially on other experts within and without the DoD, to satisfy key protection requirements.

Next, the Army must train the force to execute IO. Training the soldier will be of little value if his leaders do not completely understand IO and its effects it on warfare. Training Army leaders on IO throughout all levels of command is critical for success on future battlefields, especially as the digitization of newer equipment makes timely information more relevant. To remain effective, the Army must understand threat capabilities and not underestimate an adversary's ability to use advanced technology to harm our forces with something less than lethal force. Knowing when you are under attack and establishing indications and warning procedures are paramount. It should be second nature for Army system administrators to detect an intrusion and deal with such problems.

Training in difficult IO conditions will help develop strategies for assuring continuous operations. IO training objectives must address questions of transfer control for disabled systems and viable recovery plans. Evaluations of "firewalls" and other prophylactic efforts must be conducted. Learning how to assess the denial of services in

terms of cost is significant when one considers the impact of possible future legislation. Improving the practice of defensive measures from lessons learned in training will help establish doctrine that can then be included in future training and operational planning.

As the Army focuses on modernization it cannot allow IO to become marginalized or regarded as “just another option.” A coherent approach would ensure that the requirements and acquisition process integrate all the battlefield operating systems. To ensure protection, the Army should research all evaluated commercial product listings prior to purchasing any BOS equipment. Various agencies evaluate commercial products based on different criteria and procedures. The Army could evaluate these reports relative to commercial product functionality, level of assurance, performance, and quality. The Army should also develop standard BOS equipment listings to be purchased over the short and long term after analyzing product availability, interoperability, and evaluation results.

The JCS IW-D critical elements, “integrity, authentication, non-repudiation, availability, and confidentiality,” need to be part of the total Army modernization and BOS acquisitions plans. NSA has developed the Multilevel Information Systems Security Initiative (MISSI) program. FORTEZZA<sup>52</sup> is a key component of the MISSI architecture. FORTEZZA technology, currently available, guarantees four of the five JCS critical elements - all but availability. FORTEZZA integrates state-of-the-art cryptography onto a PCMCIA card which can be used with the latest computer hardware and software. The Army can easily integrate FORTEZZA into its BOS modernization plan, since FORTEZZA is available for procurement directly from a variety of

contractors. No additional research and developmental costs are required; however, the Army needs to develop and offer proper FORTEZZA training - along with certificate management infrastructure issues and electronic key management employment.

Lastly, the Army can address the fifth JCS element, availability, through developing advanced technologies and partnerships with industry and other government agencies. Some technologies that would serve Army needs include: redundant power supplies and other key information system components; alternate means of routing and carrying time-sensitive critical traffic; anti-spoofing and anti-tampering techniques and technologies; and advanced sensing and intelligent mechanisms that alert users of upcoming potential system failures. The Army has no clear strategy or standard approach for incorporating these advanced technologies into its BOS modernization plan. The Advanced Research Program Agency (ARPA) has substantial funding to support denial of service or availability technologies. The Army can best serve itself by forming a partnership with ARPA to transition the technology into its BOS modernization plan.

## **CONCLUSION**

America is vulnerable to the IW threat. No longer can our government, businesses, and military operations isolate themselves from one another. They must work together to protect information -- a resource that is quickly becoming critically important to America. To do nothing on one level would jeopardize our quality of life; in more serious cases inaction could threaten national security. Thus far our policymakers have taken prudent measures to minimize the risks. They have developed policies and

strategies to gain better understanding of IO and threats to current systems. Prudent steps have been taken to protect our information systems within limits. Current policy is adequate. But our stated objective to win the information war clearly expresses our intentions and looks to expand the IO mission.

The current policy is feasible because America has the capability to see to it that it is implemented. Success may be hampered only by how fast information dominance can be achieved. The cost is acceptable, not prohibitive. With reasonable amounts of money and expertise dedicated to maintaining a focus on information, the policy's objectives can be attained. As the world leader and given our extensive dependence on information and information systems infrastructure, America must ensure the protection of information and thus ensure that information continues to enhance our way of life.

Our nation's IW policy seems to be sound. The ends, ways, and means are balanced; the current strategy provides a roadmap for success. The risk assessments clearly indicate that it is unacceptable to ignore the threat to our information systems. Our policy is suitable, feasible, and acceptable. However, winning the information war will not be easy and simple, nor will it ever be over. Clausewitz reminds us in On War that in war no outcome is ever final.

## ENDNOTES

- <sup>1</sup> The Book of Proverbs, The Bible, Chapter 1, verses 5-7.
- <sup>2</sup> The White House, A National Security Strategy of Engagement and Enlargement (Washington, 1996), 24.
- <sup>3</sup>Ibid., 25.
- <sup>4</sup>Joint Chiefs of Staff, National Military Strategy, (Washington, 1995), ii.
- <sup>5</sup>Ibid., 15.
- <sup>6</sup>William J. Perry, Annual Report to the President and the Congress (Washington: U. S. Government Printing Office, 1996), 83.
- <sup>7</sup>Ibid., 83.
- <sup>8</sup>Ibid.
- <sup>9</sup>Martin C. Libicki, What is Information Warfare (Washington: U. S. Government Printing Office, 1995), ix.
- <sup>10</sup>Peter Costantini, "Technology-Information: Could Cyberwars be another Pearl Harbor?" 9 August 1996, [http://iac-insite.com/cgi\\_appl.cgi/9/2/4109/4?xrn\\_7](http://iac-insite.com/cgi_appl.cgi/9/2/4109/4?xrn_7).
- <sup>11</sup>Ibid.
- <sup>12</sup>Ibid.
- <sup>13</sup>Ibid.
- <sup>14</sup>Christopher J. Dorobek and William Jackson, "DOJ incident exposes Web insecurities," Government Computer News 9 September 1996, 1.
- <sup>15</sup>Associated Press, "Pentagon closes its Web sites after hacking intrusion," Baltimore Sun, 31 December 1996, sec. A, p. 6.
- <sup>16</sup>Kurt N. Molholm, "Information Highway around the Defense Community," Defense 96, no. 6 (1996): 43.
- <sup>17</sup>Associated Press, Baltimore Sun, 6A.
- <sup>18</sup>Neil Munro, "Cyberspace Guards Quietly Snuff Out Hacker Attacks," Washington Technology 21 November 1996, p. 1.
- <sup>19</sup>Constantini, 1.
- <sup>20</sup>Ibid., 2.
- <sup>21</sup>Department of Defense, Directive 3600.1, Information Operations and Information Warfare, (Washington: DoD, 5 September 1996).
- <sup>22</sup>Perry, 237.
- <sup>23</sup>Perry, 86.
- <sup>24</sup>Periscope Daily News Capsules, "U.S. - JWID War Games Will Test battlefield C4I Capabilities," Periscope Daily News 6 August 1996.
- <sup>25</sup>Thomas Kaneshige, "CIA plans cyberwar defense center," [http://iac-insite.com/cgi\\_appl.cgi/9/2/41029/4?xm\\_17](http://iac-insite.com/cgi_appl.cgi/9/2/41029/4?xm_17), 1 August 1996.
- <sup>26</sup>Steve Lohr, "High-Tech Information Warfare," Wall Street Journal, 30 September 1996.
- <sup>27</sup>Ibid., 3.
- <sup>28</sup>Pat Cooper, "Information Warfare Operations Require Intelligence Boost," Defense News, 9-15 September 1996.

<sup>29</sup>Wall Street Journal, "DoD Urges Information Czar Appointment," Wall Street Journal 6 January 1997, sec. B, p. B2.

<sup>30</sup>John M. Shalikashvili, Joint Vision 2010, (Washington: DoD 1996).

<sup>31</sup>John M. Shalikashvili, Information Warfare - A Strategy for Peace... The Decisive Edge in War, (Washington: DoD 1996).

<sup>32</sup>Ibid.

<sup>33</sup>Ibid., 2.

<sup>34</sup>Ibid., 8.

<sup>35</sup>Ibid., 17.

<sup>36</sup>Dennis Reimer, "Information Operations," Department of the Army Message, 041406Z Sep 96.

<sup>37</sup>Dennis Reimer, Army Vision 2010, (Washington: U. S. Department of the Army, 1996), 1.

<sup>38</sup>Ibid., 9.

<sup>39</sup>Ibid., 10.

<sup>40</sup>Ibid., 17.

<sup>41</sup>Reimer "IO", DA Msg.

<sup>42</sup>Dennis Reimer, "Information Operations Intent and Strategy" (corrected copy), Department of the Army Message, 031948Z Sep 96.

<sup>43</sup>Clarence A Robinson, Jr., "Army Information Operations Protect Command and Control," Signal, July 1996, 47.

<sup>44</sup>Ibid., 48.

<sup>45</sup>Ibid.

<sup>46</sup>"Rapid Technology Growth Spawns Land Information Warfare Activity," Signal July 1996, 53.

<sup>47</sup>Ibid., 52.

<sup>48</sup>Robinson, 47.

<sup>49</sup>Signal, 54.

<sup>50</sup>Office of the Deputy Chief of Staff for Intelligence, Intel XXI, Vision for the 21st Century, (Washington: U. S. Department of the Army 1996), 3.

<sup>51</sup>Ibid., 8.

<sup>52</sup>FORTEZZA is the cornerstone of Multi-Level Information System Security Initiative (MISSI) technology. It is a "smart card" designed to provide a customer with data integrity, authentication, non-repudiation, confidentiality and availability.

## BIBLIOGRAPHY

Associated Press. "Pentagon closes its Web sites after hacking intrusion." Baltimore Sun, 31 December 1996, sec. A, p. 6.

Bellin, David., and Gary Chapman. Computers in Battle-Will They Work? New York, NY: Harcourt Brace Jovanovich, Inc., 1987.

Campen, Alan D. The First Information War. Fairfax, VA: AFCEA International Press, 1992.

Campen, Alan D., Douglas H. Dearth and R. Thomas Goodden. Cyberwar: Security, Strategy and Conflict in the Information Age. Fairfax, VA: AFCEA International Press, 1996.

Clausewitz, Carl von. On War. Translated and edited by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Cooper, Pat. "Information Warfare Operations Require Intelligence Boost." Defense News, 9-15 September 1996.

Costantini, Peter. "Technology-Information: Could Cyberwars be another Pearl Harbor?" <[http://iac-insite.com/cgi\\_appl.cgi/92/4109/4?xrn\\_7](http://iac-insite.com/cgi_appl.cgi/92/4109/4?xrn_7)>. 9 August 1996.

Defense Intelligence Agency. Vector 21-A Strategic Plan for the Defense Intelligence Agency. Washington: U. S. Government Printing Office, 1996.

Defense Science Board Task Force. Report of the Defense Science Board Task Force on Information Warfare-Defense. Washington: U. S. Department of Defense, November 1996.

Dorobek, Christopher J., and William Jackson. "DOJ incident exposes Web insecurities." Government Computer News, 9 September 1996.

Fowler, Charles A., and Robert F. Nesbit. "Tactical Deception in Air-Land Warfare." Journal of Electronic Defense 18, no. 6 (1995): 37-44.

Harknett, Richard J. "Information Warfare and Deterrence." Parameters 3 (Autumn 1996): 93-107.

Information Warfare: Legal, Regulatory, Policy and Organizational Considerations For Assurance. 2d ed. Washington: U. S. Government Printing Office, 4 July 1996.

Joint Chiefs of Staff. Information Warfare-A Strategy for Peace...The Decisive Edge in War. Washington: Joint Chiefs of Staff, 1996.

Joint Chiefs of Staff. Joint Doctrine for Command and Control Warfare (C2W). Joint Publication 3-13.1. Washington: Joint Chiefs of Staff, 7 February 1996.

Joint Chiefs of Staff. Joint Vision 2010. Washington: Joint Chiefs of Staff, 1996.

Joint Chiefs of Staff. National Military Strategy. Washington: Joint Chiefs of Staff, 1995.

Kaneshige, Thomas. "CIA plans cyberwar defense center." <[http://iac-insite.com/cgi\\_appl.cgi/92/4109/4\\_17](http://iac-insite.com/cgi_appl.cgi/92/4109/4_17)>. 1 August 1996.

Libicki, Martin C. What Is Information Warfare? Washington, DC: National Defense University Press, 1995.

Lohr, Steve. "High-Tech Information Warfare." Wall Street Journal, 30 September 1996.

Molander, Roger C., Andrew S. Riddile and Peter A. Wilson. "Strategic Information Warfare: A New Face of War." Parameters 3 (Autumn 1996): 81-92.

Molholm, Kurt N. "Information Highway around the Defense Community." Defense 96, no. 6 (1996): 43.

Munro, Neil. "Cyberspace Guards Quietly Snuff Out Hacker Attacks." Washington Technology, 21 November 1996, p. 1.

National Defense University. Strategic Assessment 1996 Instruments of U. S. Power. Washington: National Defense University Press, 1996.

Periscope Daily News Capsules. "U. S. - JWID War Games Will Test Battlefield C4I Capabilities." Periscope Daily News, 6 August 1996.

Perry, William J. Annual Report to the President and the Congress. Washington: U. S. Government Printing Office, March 1996.

"Rapid Technology Growth Spawns land Information Warfare Activity." Signal, July 1996, 53.

Reimer, Dennis General. "Information Operations." Department of the Army Message, 041406Z September 1996.

Reimer, Dennis General. "Information Operations Intent and Strategy." Department of the Army Message (Corrected Copy), 031948Z September 1996.

Robinson, Clarence A. "Army Information Operations Protect Command and Control." Signal, July 1996, 47.

Sullivan, General Gordan R., and Colonel James M. Dubik. Envisioning Future Warfare. Fort Leavenworth, KS: U. S. Army Command and General Staff College Press, 1995.

The Bible. The Book of Proverbs, Chapter 1, verses 5-7.

The White House. A National Security Strategy of Engagement and Enlargement. Washington: U. S. Government Printing Office, 1996.

Toffler, Alvin., and Heidi Toffler. War and Anti-War. Boston, MA: Little, Brown and Company, 1993.

U. S. Department of the Army. Army Military Intelligence-Vision for the 21st Century. Washington: U. S. Department of the Army, 1996.

U. S. Department of the Army. Army Vision 2010. Washington: U. S. Department of the Army, 1996.

U. S. Department of the Army. Information Operations. Army Field Manual 100-6. Washington: U. S. Department of the Army, August 1996.

U. S. Department of Defense. Information Operations and Information Warfare. DoD Directive 3600.1. Washington: U. S. Government Printing Office, 5 September 1996.

Wall Street Journal. "DoD Urges Information Czar appointment." Wall Street Journal, 6 January 1997, sec. B, p. B2.

West, Togo D. Jr., and General Gordan R. Sullivan. United States Army Vision Posture Statement FY96. Posture Statement presented to the 104th Cong., 1st session Washington: U. S. Department of the Army, 1995.

West, Togo D. Jr., and General Dennis J. Reimer. United States Army Vision Posture Statement FY97. Posture Statement presented to the 104th Cong., 2nd session Washington: U. S. Department of the Army, 1996.